How to Protect against E-mail Fraud

What is Phishing and Spamming?
Phishing is the practice of luring unsuspecting Internet users to a fake website by using authentic-looking e-mail with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack. A website replica is created for fooling unsuspecting Internet users into submitting personal or financial information or passwords. Phish e-mails are also referred to as spoofs.
Spamming is unsolicited or junk e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups. They usually offer dubious products, get-rich-quick schemes, or illegal services.
Being in a college environment, it may seem that we are more susceptible to these types of attacks but there are techniques for reducing the number of these e-mails. We'll give you some valuable tips to identify these emails, implement best practices, what to do with these emails, and how to report them.

How to Identify if an E-mail is a Fraud?
The first step in combating the onslaught of spam is to know it when you see it. If in the subject line it is offering you a lower mortgage rate or free money, you know it is spam. But be careful, because spammers often use tricks to make the subject line something you might click on, such as "FWD: great punch line." So, even if the subject looks harmless, your best bet is to just delete it if you don’t recognize the address.
Unfortunately, it can be hard at first glance to tell if a message is fraudulent. For example, many spoofed e-mail messages link to real company logos. You should be cautious of:

- **Requests for personal information in an e-mail message.** Most legitimate businesses have a policy that they do not ask you for your personal information through e-mail. Be very suspicious of a message that asks for personal information even if it might look legitimate.

- **Urgent wording.** Wording in phishing e-mail messages is usually polite and accommodating in tone. It almost always tries to get you to respond to the message or to click the link that is included. To increase the number of responses, criminals attempt to create a sense of urgency so that people immediately respond without thinking. Usually, fake-e-mail messages are NOT personalized, while valid messages from your bank or e-commerce company generally are personalized. The following is an example from a real phishing scheme:

Dear valued bank customer, it has come to our attention that your account
information needs to be updated due to inactive member, fraud, and spoof reports. Failure to update your records will result in account deletion. Please follow the link below to confirm your data.

**Fake links.** In HTML-formatted messages, the links that you are urged to click contain all or part of a real company’s name and are usually “masked,” meaning that the link you see does not take you to that address but to a different address, usually a spoofed website.

**Message body is an image.** To avoid detection by spam filters, fake e-mail messages used in phishing schemes often use an image instead of text in the message body. If the spam message uses real text, most junk e-mail filters will likely move the message to the junk e-mail folder. The image in the message is usually a hyperlink. You can tell because when you use your mouse to rest the pointer on the message body, the pointer becomes a hand indicating a hyperlink.

**Attachments.** Many phishing schemes ask you to open attachments, which can then infect your computer with a virus. Don’t open attachments in suspicious e-mail messages. Any attachment that you want to view should be saved first, and then scanned with an up-to-date anti-virus program before you open it.

**Promises that seem too good to be true.** Use common sense and be suspicious when you are offered money or discounts that seem too good to be true.

**Best Practices to Help Protect Yourself from Fraud**

Follow these guidelines to help lower your risk of getting junk e-mail:

**Monitor your transactions.** Review your order confirmations and credit card and bank statements as soon as you receive them to make sure that you’re being charged only for transactions you have made. Immediately report any irregularities in your accounts by dialing the number shown on your account statement. Using just one credit card for online purchases makes it easier to track your transactions.

**Take advantage of the Junk E-mail Filter in Outlook 2003.** The junk e-mail filter evaluates a message to determine the probability that it is junk e-mail. By default, this filter is set to a low setting that is designed to catch the most obvious junk e-mail. Any message that is caught by the filter is moved to a special junk e-mail folder, where you can retrieve or review it at a later time. **NOTE:** If you increase the setting, you will need to check the junk e-mail folder more frequently to remove any regular e-mail that might have been placed there by mistake.

**Block images in HTML messages that spammers use as Web**
beacons. A web beacon can be a graphic image, linked to an external Web server that is placed in an HTML-formatted message and can be used to verify that your e-mail address is valid when the message is opened and images downloaded. By default, Outlook is set to block automatic picture downloads. To verify what your automatic download settings are, on the Tools menu, click Options. Click the Security tab, and then click Change Automatic Download Settings. Verify that the Don’t download pictures or other content automatically in HTML e-mail check box is selected.

Use multiple e-mail addresses for different purposes. You might set up one for personal use to correspond with friends, family, or colleagues, and use another for more public activities, such as requesting information, shopping, or for subscribing to newsletters, discussion lists, and newsgroups.

Watch out for check boxes that are already selected. When you buy things online, companies sometimes add check boxes (already selected!) to indicate that it is fine to sell or give your e-mail address to other businesses (third parties). Clear the check box so that your e-mail address won’t be shared.

What to do with Spam once it has been Identified
Once you’ve identified a message as spam, don’t just delete it. Here’s what to do (and what not to do) when you have unwanted e-mail.

Identify spam to your e-mail provider. E-mail providers stop significant amount of spam using e-mail filters. It will funnel unwanted messages into a bulk e-mail or junk mail folder. Goucher has a server dedicated just for blocking spam. It catches thousands of unwanted e-mails a week but, some do get through. So, if you receive spam, place the e-mail message in the Spam public folder.

Never open an attachment from a suspicious e-mail. It may contain a virus that could infect your computer. To compound the damage, it could duplicate the virus and send it to everyone in your e-mail address book, potentially infecting their computers as well. Goucher’s e-mail server is protected by anti-virus software which removes most potentially infected attachments before you receive an e-mail. You may notice some spam e-mails that have attachments entitled “eTrust Antivirus ScanReport.Txt”. That lets you know that the infected attachment has been removed. However, new viruses are created every day and a virus may slip through the cracks so be diligent about watching out for suspicious attachments.

Don’t forward an unknown e-mail. Sometimes spam will have a fake
“To” or “From” field. Since it appears that the e-mail was erroneously sent to you, the spammer hopes you’ll read it and helpfully forward it along. Please do not forward suspicious e-mails.

**Resist the temptation to unsubscribe.** Sometimes clicking a link that promises to unsubscribe you lets the spammer know that your e-mail address is valid, which means you might be spammed even more.

**How to Report Fraud**

If you believe that you have received fraudulent e-mail messages you can report the problem to the following groups:

**Goucher Help Desk.** You can contact us via phone (x6322) or e-mail (helpdesk@goucher.edu) to let us know if you are receiving any suggestive or unwanted e-mails. You can also put these e-mails in our SPAM folder. This helps our spam server to improve the blocking of these types of e-mails in the future. To move e-mails to the SPAM folder, click on the **Folder list** icon to reveal **Public Folders**. Click on **All Public Folders** to show the list of folders. Then drag the e-mail from your inbox to the **SPAM** folder.

**Federal Bureau of Investigation (FBI).** The [FBI: Internet Fraud Complaint Center (IFCC)](https://www.ifcc.fbi.gov/) works worldwide with law enforcement and industry to promptly shut down phishing sites and identify the perpetrators behind the fraud.

**Federal Trade Commission (FTC).** If you believe that your personal information has been compromised or stolen, you should report the circumstances to the FTC: National Resource for Identity Theft and visit their site to learn how you can minimize the damage. For more information on how to prevent phishing scams check out the following site:

[How Not to Get Hooked by a ‘Phishing’ Scam](https://www.consumer.ftc.gov/articles/0019-phishing-scams)